Certificate

fs.usda.gov | Entrust Certification Authority - L1K | Entrust Root Certification Authority - G2

Subject Name

Country	US
State/Province	Missouri
Locality	Kansas City
Organization	US Department of Agriculture
Common Name	fs.usda.gov

Issuer Name

Country	US
Organization	Entrust, Inc.
Organizational Unit	See www.entrust.net/legal-terms
Organizational Unit	(c) 2012 Entrust, Inc. - for authorized use only
Common Name	Entrust Certification Authority - L1K

Validity

Not Before	Thu, 04 Jan 2024 21:06:11 GMT
Not After	Tue, 04 Feb 2025 21:06:10 GMT

Subject Alt Names

DNS Name	fs.usda.gov

Public Key Info

Algorithm	RSA
Key Size	2048

Exponent	65537
Modulus	97:87:6A:0C:24:49:77:02:07:51:EE:41:82:03:B9:A9:49:25:CB:6E:15:4…

Miscellaneous

Serial Number	5E:2B:F2:39:95:B1:1D:CC:96:22:76:E3:B8:74:27:17
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	9F:5B:9B:C8:69:21:69:7A:18:61:55:61:9C:4F:D0:0F:F6:E7:4E:74:25:3…
SHA-1	F3:53:C7:21:FF:ED:E6:42:BF:4F:2A:D4:23:A0:88:E8:7C:57:02:50

Basic Constraints

Certificate Authority	No

Key Usages

Purposes	Digital Signature, Key Encipherment

Extended Key Usages

Purposes	Server Authentication, Client Authentication

Subject Key ID

Key ID	04:5F:E7:B6:A0:4C:FC:99:5A:02:FB:86:7F:E5:26:83:47:86:6F:EA

Authority Key ID

Key ID	82:A2:70:74:DD:BC:53:3F:CF:7B:D4:F7:CD:7F:A7:60:C6:0A:4C:BF

CRL Endpoints

Distribution Point	http://crl.entrust.net/level1k.crl

Authority Info (AIA)

Location	http://ocsp.entrust.net
Method	Online Certificate Status Protocol (OCSP)
Location	http://aia.entrust.net/l1k-chain256.cer
Method	CA Issuers

Certificate Policies

Policy	Certificate Type (2.23.140.1.2.2)
Value	Organization Validation

Embedded SCTs

Log ID	E6:D2:31:63:40:77:8C:C1:10:41:06:D7:71:B9:CE:C1:D2:40:F6:96:84:…
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Thu, 04 Jan 2024 21:06:11 GMT
Log ID	A2:E3:0A:E4:45:EF:BD:AD:9B:7E:38:ED:47:67:77:53:D7:82:5B:84:94:…
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Thu, 04 Jan 2024 21:06:11 GMT
Log ID	4E:75:A3:27:5C:9A:10:C3:38:5B:6C:D4:DF:3F:52:EB:1D:F0:E0:8E:1B:…
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Thu, 04 Jan 2024 21:06:11 GMT